

IN THE ABSTRACT:

Please amend the abstract as follows:

Securely storing a public key for encryption of data in a computing device by using a user-specific key pair which is securely stored in the computing device, including receiving a target public key corresponding to a target device, obtaining a user-specific key pair from a secure registry, using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key, storing the target key verifier and the target public key in a storage area, retrieving the target key verifier and the target public key from the storage area, applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key, and encrypting data with the target public key, ~~in the case that the if~~ authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device.